ORIGINAL

1 JAMES R. BUSSELLE (SBN 75980)
   THOMAS E. MOORE III (SBN 115107)
2 MARY O'BYRNE, (SBN 121067)
   TOMLINSON, ZISKO, MOROSOLI & MASER
3 200 Page Mill Road, Second Floor
   Palo Alto, California 94306
4 Telephone: (415) 325-8666

5 Attorneys for Defendant
   RSA Data Security, Inc.

6

7

8   UNITED STATES DISTRICT COURT

9   NORTHERN DISTRICT OF CALIFORNIA

10

11 ROGER SCHLAFLY,   )   CASE NO.: C 94 20512 SW (PVT)
)
12   Plaintiff,   )   DECLARATION OF CLAUS P.
)   SCHNORR IN OPPOSITION TO
13 vs.   )   PLAINTIFF'S MOTION FOR
)   PARTIAL SUMMARY JUDGMENT
14 PUBLIC KEY PARTNERS and RSA DATA)
    SECURITY, INC.,   )   DATE: December 6, 1995
15   )   TIME: 10:00 a.m.
               Defendants.   )   BEFORE: Hon. Spencer
16 _____)   Williams

17

18   I, Claus P. Schnorr, declare:

19   1.   I am one of the inventors of U.S. Patent No.

20 4,995,082, "Method for identifying Subscribers and for Generating

21 and Verifying Electronic Signatures in a Data Exchange System." I

22 have personal knowledge of each and every fact set forth below

23 and can competently testify thereto.

24   2.   I applied for a U.S. patent on my invention on or

25 about February 23, 1990. The U.S. patent was issued as U.S.

26 Patent No. 4,995,082, on February 19, 1991.

27   3.   Claim 5 of my patent describes a general method for

28 preprocessing signatures that are based on a discrete logarithm.

SCHNORR DECL. IN OPP. TO PLTF'S   -1-
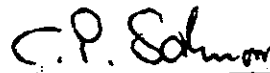MOT. FOR PART. SUM. JUDG.,
CASE NO. C94-20512-SW
                                                                47600.1

FILED
Nov 15 3 31 PM '95
RICHARD W. WIEKING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CA. S.J.

1 After my patent was issued, Peter de Rooij found weaknesses in

2 two specific instances of the general method described in Claim

3 5. These specific weaknesses do not apply to the general method

4 described in the patent. However, the general method must be

5 applied with some care to preserve the security of the digital

6 signatures.

7   4. After de Rooij published his work, my students and I

8 further developed the general method described in Claim 5. We

9 have examples of the general method which are efficent and

10 provably secure. Some of these methods are described in the

11 master's thesis of my student Johannes Merkle, "On Schnorr's

12 Preprocessing Method," which was published in 1994.

13   5. The other features of my invention are independent of

14 the preprocessing method described in Claim 5. In particular,

15 the digital signature generation method described in Claim 6 can

16 well be used without the particular preprocessing method of Claim

17 5. Therefore, the validity of the other claims is not related to

18 the utility of Claim 5.

19   I declare under penalty of perjury under the laws of the

20 United States of America that the foregoing is true and correct.

21 Executed on November 14, 1995 at Frankfurt, Germany.

22

23   _____
                                       Claus P. Schnorr
24

25

26

27

28